Fall 2018

Implementing CIS Cybersecurity Controls for the Department of Residence, Iowa State University

Vishwas Kaup Vijayananda
Iowa State University

Implementing CIS Cybersecurity Controls for the Department of Residence, Iowa State University

Creative component for
Master of Science in Information Systems
Iowa State University

Vishwas Kaup Vijayananda

Supervised by:
Professor James Davis

November 2018

Outline

Acknowledgement

I would like to express my gratitude to the staff members from Iowa State University's Department of Residence for being cooperative in every step of the process.

Special thanks to Dave Symmons, Tim Wilson, Barrett Ford and a fleet of undergraduate students (Kieffer, Brendon and Ross) for helping me out in bringing this project to real life.

I would also like to thank professor James Davis from Iowa State University's College of Business for sharing his thoughts and opinions on the project. This helped me in dealing with the problem in a matured manner, and his experience gave me a chance to look at the issue from both a managerial and a technical perspective.

I have learnt a lot from this project, and it wouldn't have been possible without the help and support of all these people. I am truly grateful to them, and I hope that this project receives the same kind of support in the future years to come.

Thank you,
Vishwas

Abstract

The Department of Residence (DoR) at Iowa State University houses over 13,000 students, and employs over 300 staff members.

Department of Residence's IT team is in charge of taking care of Information systems assets (data, servers, systems, IP Phones, networking devices, VMs and printers) that are used by the students and the staff members.

It is imperative for the DoR to reduce total IT spending, and also to secure the infrastructure to keep hackers and cyber criminals at bay.

Various cybersecurity solutions were discussed, and we finally decided to implement CIS-Security Framework. It was one of the most effective ways to tackle the needs of the Department. The Framework consists of a set of actionable Controls, and realizing just a few of these controls had a big impact on the department's IT spending and infrastructure security. Two controls which were implemented are briefly mentioned below-

The first cybersecurity control is to have an inventory of all the authorized and unauthorized hardware devices in the network, so that only authorized devices are given access. This includes a list of active data jacks that are in use as well as staff, student and departmental assets.

The second cybersecurity control is having an inventory of all the authorized and unauthorized software installed in all the systems, so that only authorized software can be installed and executed.

For now, implementing just the first two controls is enough to meet the financial and security goals of the Department. This work has bolstered the department wide security, and has an estimated annual savings of $200,000 per year. But in the future, it will be important for DoR to implement the rest of the Controls to compete with the changing threat landscape.

Introduction

Iowa State University has a total student population of over 36,000. Out of this total, over 13,000 students live in the Iowa State University's Residence Halls. There are 13 such Residence Halls spread across the campus, and they are all managed by the Department of Residence (DoR).

Department of Residence's IT Team is responsible for purchasing, renting, administering and securing the Information system assets (data, data jacks, servers, systems, IP Phones, network devices, VMs and printers) that belong to the Department of Residence.

Because of financial restrictions, the Department of Residence rents most of these assets from Iowa State University's Information Technology Solutions Center (ITS), and pays for it on a monthly basis. This sums up to a total of over $2M annually.

The list of devices and data jacks which are rented has not been updated recently, and many of these devices are either not in use or are not to be found. It means that the DoR is not only spending in excess, but it also has a large attack surface open for security breaches. This poses a serious security threat as anyone who can get access to these unused devices or ports can cause harm to the University.

Also, since DoR holds confidential data related to the students, staff and the University, a data breach could be very costly. It can damage the University's reputation and even cripple its daily functioning. Hence it is crucial for the department to protect the data it has by increasing the overall security.

By implementing a good security program, the department can not only spend less on unwanted resources, but also improve the security across the network. It can then focus on providing better service for the students, directly impacting the quality of life in Residence Halls. This will eventually help the department in selling better in the years to come.

To reach these business goals of the department, the DoR's IT Team decided to implement CIS Security Framework across the network. This decision was made based on my previous experiences working closely with the CIS security Controls, the engineering practicality it provided and the overall ease of implementation.

I am a graduate assistant working with the Department of Residence's IT Team. With the help of Tim Wilson, Dave Simmons, and a fleet of undergraduate students, we were

able to successfully implement the popular CIS Cybersecurity Framework to meet the end objectives of the Department.

Problem Statement

From the initial research that we did, it was clear that the department was not just carelessly spending its money on resources that are not required, but it also did not adhere to any set of best practices to have and maintain a secure network. Because of inefficiencies and lack of maintenance in the network, the whole infrastructure was obsolete and vulnerable to external attacks. There was no system in place to secure the existing architecture and to bring the excessive spending under control.

There had to be a strategy for the Department so that it can meet its financial and security needs. By cutting down excessive IT spending and paying only for assets that are in use, the Department will be financially more stable and can start buying assets of its own instead of relying on ITS. This is the financial goal of the Department. The security goals can be met by creating a list of managed hardware and software components that are present in the network, and keeping this updated with every addition or removal of these components. This can be achieved by implementing/ adhering to a best practice security framework in the department, in turn reducing the security risks posed on the network.

Though the project if done right will save the Department money and bolster the overall security, investing fresh resources for this project was a big obstruction. There was no dedicated annual budget for the program, and the funds had to come from the main IT budget. Several constraints arose because of this reason.

There was no dedicated workforce hired to manage this project. Instead of having Subject Matter Experts working closely with a team of engineers, we were a few College students coordinating with each other and working with one other full-time staff from the IT team.

As college students, we had restricted access to the department's information and assets. To get access to anything, it must first be approved by other teams within the Department. This is a long and time-consuming administrative process with low visibility into the status of the issue. As a result, we had to exchange multiple follow up emails with several internal teams before we obtained the right information. This affected the flow of the work and added to the complexity of the project.

Also because of the financial restrictions, the management was not in favor of buying proprietary tools and technologies. This was seen as excessive spending, and it restricted the IT team's options to a limited number of open source alternatives. Open source software comes free of cost, but has its own set of disadvantages. It does not have a vendor support, so it is difficult to find solution to a problem as it arises. Also

the configuration and setting up is not straightforward, and it takes time and effort to understand the software before using it. It is not an off-the-shelf solution. In addition to all this, these tools come with limited functionalities as opposed to their paid/supported versions. As a result, we were left with complicated engineering problem, and was the IT Team's worry to come up with a workable solution.

In spite of having many restrictions, it was required for the Department's IT Team to come up with a solution to effectively cut down excessive costs to buy its own assets, and to improve the security standards to maintain a clean network throughout the Department.

Different Solutions

To accomplish project goals with the constraints of spending only for what's required and securing the overall infrastructure, several meetings were held to talk about different cost saving solutions, security frameworks, device vendors, opensource tools and related technologies.

From these discussions, it was clear that we needed to implement a department wide security framework [7] to reduce the risks and vulnerabilities posed on the infrastructure. A Common Security Framework [8][1] can be explained as a set of well documented policies and guidelines that can be used by the employees to govern the implementation and management of an organization's overall security. This can be served as a blueprint as it contains step by step processes that can be utilized by the staff members to define, document and prioritize security related tasks, issues and solutions. Adhering to the set of Best Practices laid out by the Framework will build a strong defense across the department, and cuts down unnecessary costs at the same time- meeting both the financial and security goals of the Department.

There were several such Industry recognized frameworks to begin with. NIST Cybersecurity Framework[2], IS0 27001[1], COBIT-5[11] and CIS Security Controls[5] were all different options that were taken into consideration. Though these frameworks had a lot of concepts in common, they had their own ways of tackling the problem.

NIST Cybersecurity Framework [2] talks about the planning and implementation of enterprise security from a defense point of view in an organized way. It consists of three different parts: The framework Core, the Implementation part and the Framework Profiles. The Core talks about the five primary functions of the framework-

- Identify- Identify the data, the value in it and assets present in the network.
- Protect- Upon evaluating the value of the assets, protect them based on their criticality
- Detect- Place defense mechanisms to detect malicious activity in the network
- Respond- How an organization should respond if and when an adversity occurs
- Recover- Recovery mechanisms to retrieve lost data

The Framework implementation tiers gives a context on how an organization views cybersecurity based on factors such as the total value that's created, feasibility of the solution and the total impact on the organization. They go from Tier-1 through to Tier-4 based on the cybersecurity awareness within the organization. The Framework Profiles talks about alignment of the core principles of the organization with the cyber security strategy and the implementation tiers. Together, it enables the top

management in the organization to identify the gaps, and understand what has to be implemented from a managerial point of view.

ISO 27000 is a family of internationally recognized standards used to keep as organization's information system assets secure from cyberattacks. ISO 27001[1] was one such cybersecurity strategy that was seen as a potential solution for the problem in hand at the DoR. It lists a set of IT standards to protect the assets in a network by ensuring Confidentiality, Integrity and Availability of the data. It follows a risk based approach where all the adversaries are seen as potential risks to the assets within an organization. After this assumption, preventive measures or safeguard controls can be set up to protect these data/assets. These preventive measures are usually in the form of policies, procedures and best practices and their implementation requires the involvement of top level management. Organizations use ISO 27001 primarily to meet the regulatory requirements of the company and to achieve marketing advantage.

COBIT 5 [6] is a business framework for the governance and management of enterprise IT. It is an umbrella term as it encompasses other frameworks such as ITIL, COBIT-4 and ISACA's Val IT and Risk IT. It gets into details of business process management, technology management, quality and reliability control- enabling an enterprise's top management to evaluate and get an end-to-end view of the total value that is created by IT. It also doesn't include a lot of technical documentation, but is recommended for IT governance, Risk assessment and IT Compliance.

CIS Security Controls [5] are a prioritized set of controls that can be implemented to either secure an existing infrastructure or to build security from the scratch. These controls are solutions built from an attacker's point of view. It gets into precise technical content, and provides a step by step process to implement an enterprise-wide defense.

After careful comparisons and analysis, we decided to go ahead with CIS Security Framework to implement security across the Department. By bolstering the existing security needs, the CIS Security Framework enabled us to pinpoint and cut down unnecessary spending to meet the Department's overall business needs.

Apart from being one of the most effective ways to build security in an infrastructure, there were other important reasonings to be made before choosing to go with CIS Security Framework. Factors such as the relevance it had to today's threatscape, the technical granularity it provided, and the ease of implementation were all taken into consideration. These factors are discussed in detail in the upcoming section.

CIS Controls

What are they?

Center for Internet Security (CIS) [9][5] is a non-profit Organization founded in 2000 with an intention to develop and maintain best practice solutions for an effective enterprise cyber defense. They provide solutions that meet the globally recognized standards and best practices to secure IT systems and data from today's cyber-attacks.

The CIS Security Framework consists of list of well-defined Security controls. According to the official website, CIS Security Controls can be defined as a set of planned and prioritized actionable steps that can be taken by an organization to either implement cybersecurity from the scratch or to assess and improve an existing security architecture.

How many in total? Why CIS?

With a total of 20 Controls, it heavily advocates the philosophy of Defense in Depth to detect, prevent and secure the Information Systems from external attacks.

They are built on the learnings of actual attacks and responses from the effective defense systems. It reflects the combined knowledge of security experts from across the industry, government and academia from across the globe. It is also continually monitored and updated to ensure that these controls are in pace with the evolving threatscape, so that the organization has the most effective way to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

A study from Seals and Tara in May 2017 [4] showed that "on average, organizations fail 55% of compliance checks established by the Center for Internet Security", with more than half of these violations being high severity issues. This figure shows us the importance and relevance these Security Controls have in today's world.

It is estimated that by implementing these controls, an organization can prevent over 85% of the common security attacks.

The most recent version of CIS Controls was released in March 2018 and is in its Version 7 [5]. The fundamental controls remain the same, but they are separated into three distinct categories: basic, foundational and organizational.

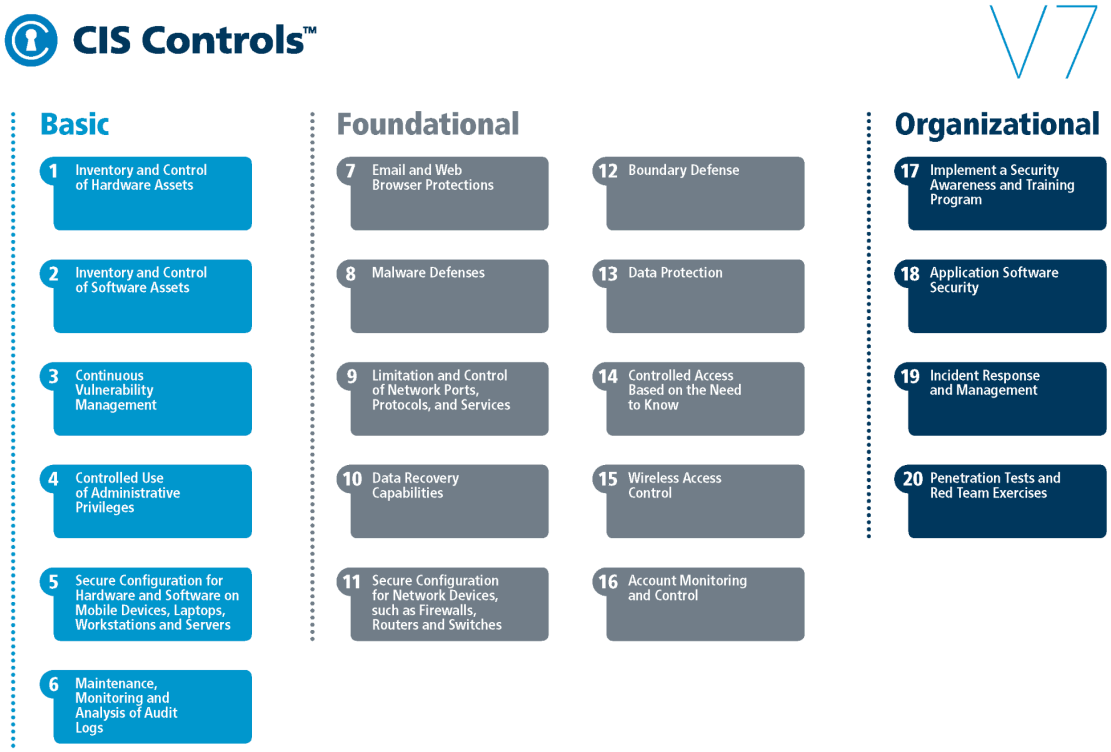
- The basic category comprises of the first six Controls 1-6 which forms the bare minimal requirements for essential cyber defense readiness. Implementing these

controls will reduce a huge part of the attack surface when a hacker is trying to break into the system.

- The foundational category contains the CIS Controls from seventh to the sixteenth. This is next step up after the basic controls and it states the set of best practices that can be followed by any organization to proactively take measures against cyber-attacks.

- The last and final Organizational category covers the last four of the CIS Controls. These controls are more focused towards the people and processes aspect of an enterprise cybersecurity.

This is graphically shown as show below



PC Credits- This image is taken from the official CIS webpage. [5]

Why these controls?

Implementing the basic Controls from 1 to 6 of the CIS Cybersecurity Framework are among first set of controls to be implemented. We decided to start with the first two

security controls because this not only lays the groundwork for the rest of the implementation, but it also gives a good understanding of the entire infrastructure.

This directly contributes to the success of the whole project. The financial goals will be met, as we can stop paying for all the unauthorized software and hardware devices in the network and instead invest this difference amount in buying our own assets. The security goals will be met by having only legit software applications and hardware devices in the network leaving very less room for vulnerable applications to be present in the system. This tightens the security by eliminating the risk of having an exploit in an unknown application in an unknown host.

The controls also enable us to identify the number of unused active data jacks in the network. By shutting them off and keeping only the ones that are necessary, we are spending less and effectively reducing the overall attack surface of the network. This makes the whole infrastructure a lot more secure.

Just by implementing the first two of the CIS controls, we were able to tackle both the financial and the security goals of the project. This is one of the main reasons for us to choose CIS Cybersecurity framework. Also, unlike other frameworks which vaguely describes different aspects of an enterprise security in a theoretical manner, CIS Security Framework gets the job done in an accurate and a hands-on practical manner. It gets into step by step technical details, which is easy to understand and simple to implement.

After taking into account of all these considerations, it was a no brainer for us to choose CIS Security Framework over any other alternatives. The details of the two controls which were implemented are discussed in the following section.

Comparison Chart

	Relevance	Simplicity in understanding	Technical Granularity	Ease of Implementation
NIST	a few inches deep but mile wide	Wide overview of Information Security	Does not get very technical	Several Steps Involved
ISO 27001	Somewhat relevant but not prescriptive	Risk based approach	More about Processes and Policies	Requires top management's involvement
COBIT-5	Not relevant to our requirements	Vast IT Governance	Business Processes and management	N/A
CIS Controls	Custom made	Simple!	Precise technical content	Straightforward and easy

CIS Control- 1

What is it?

For us to implement Cyber security in an enterprise, the first step is to have an inventory of all the hardware assets in the network. According to the official CIS documentation, this control is described as:
"Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." [5]

How does CIS Control-1 improve the network security?

When an attacker wants to compromise a network, the first step is to continuously scan the target network for vulnerable devices that are not updated with the latest patches and are still vulnerable to external attacks.

These devices can be new to the infrastructure and are yet to be configured, or it could be an old device that is no longer in use but is still connected to the network or can be a BYOD Device in the network. For whatever the reason, these systems are hidden from the Network Administrator view and are not updated with the latest security patches. These devices fall under the category of unauthorized devices and they pose a serious threat to the network. [5][10]

If an attacker gets access to any of these devices, there is no saying as to what can go on from there. Not only can he compromise the data in that device, but he can also carefully plan and execute a devastating attack on the entire network.

In order to prevent this from happening, the first step is to make sure that only authorized devices are given access to the data, and all the unauthorized devices are taken off the network. The solution also includes maintaining an inventory of the approved devices, continuously monitoring the network for abnormal behavior, sending out timely OS updates and having an effective incident management process in place.

Use case

The list of the authorized devices in the network was not updated for many years. Since most of the devices are rented from another department and DoR pays for it on a

monthly basis, we had the list of devices we were paying for. Though this was not an updated list, it was a place for us to start with. We used Google Sheets to maintain this list on cloud to control and edit it from different users and different devices at the same time.

First step was to coordinate with other undergraduate students in the project and plan to physically check for these devices in the network (staff buildings and hub rooms). That way, we will know what devices are actually in the network. This eliminates many entries from the list and they fall into two categories- the ones that were found and are authorized devices which will remain active, and the ones that were not found and we don't know if they are in use or not.

For the list of devices that were not found, we ran a few tests from within our department. Using opensource tools such as Nmap, OpenVAS and Solarwinds we collected Network scan and net flow device data, and then we were able to get further clarity on weather these devices were authorized or not. The unused and unauthorized devices were then pulled out of the network.

We did the same process to data jacks that were present in all the residence halls. There were several unauthorized devices and unused data jacks in the network. These devices were then turned in to ITS saving upwards of $200,000 annually. We were successful in implementing to the first control in CIS Security Framework, and it improved the overall security of the Department.

CIS Control-2

What is it?

After cleaning the network of all the unauthorized devices, the next control focusses on making sure that only authorized software is running on all these systems. According to the official CIS documentation, the second control is described as:
"Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution." [5]

How does CIS Control-2 improve the network security?

Attackers continuously scan organizations looking for vulnerable applications which can be exploited remotely to break into the network. These vulnerable applications are usually outdated software versions which do not have latest patches installed, making them easy target for the hackers. [5][10]

By exploiting these software vulnerabilities, an attacker can launch malware to directly get access to the system. Once the attacker has this access, he can then use this as a staging point to compromise other systems in the network. This can be disastrous as once he has enough systems under his control, he can compromise confidential data, and launch an enterprise wide security attack.

However, preventive measures can be put in place to mitigate such atrocities from taking place. The system administrator must maintain an inventory of all the authorized software in all the systems in the network and make sure that the latest versions of the software is installed. The unauthorized software should be uninstalled and deleted from the systems. Having an incident response team to backup and recover the data also helps in keeping the attackers at bay.

Use case

There are over 300 staff computers across the DoR network and most of these systems are running on Microsoft Windows. Some systems were running on outdated version of the OS, some systems had no vendor supported software running, and some systems had unwanted applications running in them.

A few of the applications running in these systems was maintained in Active Directory tools, but it was not an updated version. We had to first create an inventory of all the systems in the network, and the software that is supposed to be running in these machines. This way, all the unmanaged applications that we come across can be treated as unauthorized applications and can then be deleted from the systems.

To identify all the systems running on outdated systems and applications, we ran Nessus scans and used Microsoft SCCM to detect and make an inventory of the findings. Then using SCCM, Active Directory tools and group policy management, we were able to force only the installation and execution of the authorized software in all these systems. Other unwanted applications were uninstalled and removed from the network.

Finally, towards the end, we had a set of systems running on updated and secure version of the Operating System. They were having only vendor supported applications and gave us a lot of visibility. Periodic scans were put in place to make sure that the latest version of the patches are installed as and when they are released. This increased the overall security in the systems and met the needs of the Department.

Conclusions

Final evaluations

After completing the first two controls of the CIS Security Framework, we were able to meet the financial and security goals of the project. We were able to cut down unnecessary IT costs by $200,000 and invest this money in buying devices of our own, and also in improving the standard of living in the residence halls.

By following the best security practices laid out by the framework, we were able to rid the infrastructure of outdated hardware devices and software applications and have an inventory of all the software applications and hardware devices in the network. This enabled us to tie up loose ends and strengthen the overall security in the network. We implemented a continuous monitoring process so that the list of devices and applications in the network is always up to date.

All the steps involved in this project was well documented in an easy to read word document. This was made accessible to the employees for future references.

We also started a new training program where the departmental staff were educated about cyber security and healthy internet practices. We explained how a hacker can work from a remote location to break into our personal lives or disrupt an entire business operation. This process of educating the staff is imperative and has made the whole department a lot more secure.

Though the implementation of the first two CIS Controls and educating staff members was enough to meet the departmental needs for now, it will not be enough in the future years to come. It is a must for the DoR to plan and implement the remaining four of the basic CIS Security Controls in quick succession. The remaining four controls talks about the best practices in implementing the principle of least privilege, continuous vulnerability management, secure configuration of hardware and software in the infrastructure and continuous monitoring and maintenance of audit logs. Implementing the next few processes will play a key role towards building a secure IT infrastructure.

Finally, it is worth mentioning that security is not a one-time investment. As the attackers evolve and become more sophisticated, the defenses must keep up to avoid falling as prey to their attacks. The infrastructure must be continuously monitored for loopholes and updated on the go. Staff training should take place every few months to ensure that they are aware of the latest threats from harmful intenders. Everything

takes effort to be in good shape, and cyber security is not an exception. It will only get tougher in the years to come but following secure practices will only help an organization to defend itself from these attacks.

References

1. ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, 2013

2. NIST V1.1, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018

3. Symantic, ISO27001 Information Security Management System

4. Tara Seals, InfoSecurity Magazine, May 26, 2017

5. Center for Internet Security, CIS Controls, 2018

6. Blog- COBIT-5, ISACA, November 2018, https://cobitonline.isaca.org/about

7. Blog- Dejan Kosutic, The basic logic of ISO 27001: How does information security work?, 2018, https://advisera.com/27001academy/knowledgebase/the-basic-logic-of-iso-27001-how-does-information-security-work/

8. Blog- Ron Temske, What is a Common Security Framework, Logicalisinsights, Apr 2017, https://logicalisinsights.com/2017/04/07/what-is-a-common-security-framework-csf/

9. Blog- Wikipedia, The CIS Security Controls for Effective Cyber Defense, August 2018, https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense

10. Blog- CIS Critical Security Controls, November 2018, https://www.sans.org/critical-security-controls

11. ISACA, COBIT-5, 2012